3771 Eastwood Drive
Jackson, MS 39211-6381
Phone: 601-432-8000
Fax: 601-713-6380
www.its.ms.gov

Mississippi Department of Information Technology Services

David C. Johnson, Executive Director

LOC Questions and Clarifications Memorandum

To: Solicited Vendors for Letter of Configuration (LOC) Number 46217-B dated March 1, 2021, for the Mississippi Division of Medicaid (DOM)

From: David C. Johnson

Date: March 22, 2021

Subject: Responses to Questions Submitted and Clarifications to Specifications

Contact Name: Jill Chastant

Contact Phone Number: 601-432-8214

Contact E-mail Address: jill.chastant@its.ms.gov

LOC Number 46217-B is hereby amended as follows:

1) PROCUREMENT PROJECT SCHEDULE

Task	Date
Addendum with Vendors' Questions and Answers	Monday ~~Thursday~~, March 22 ~~18~~, 2021
Proposals Due	Wednesday ~~Monday~~, March 31 ~~29~~, 2021 at 3:00 p.m. Central Time
Begin Proposal Evaluation	Wednesday ~~Monday~~, March 31 ~~29~~, 2021
Notification of Award	Monday, April 12, 2021
Begin Contract Negotiations	Monday, April 12, 2021
Installation/Delivery	On or before Friday, May 28, 2021

2) Item 5.4.10.1 is being modified to read:

Vendor shall propose two Next Generation firewalls (proposed firewalls working as a High Availability pair ~~totaling four firewalls~~).

3) Item 7.13 is being added to read:

Vendor shall determine if LAGs are required.

4) Item 7.14 is being added to read:

Vendor shall clean and streamline the current configuration.

5) Item 7.15 is being added to read:

Vendor shall provide off-peak hours for cut-over. DOM will coordinate to ensure but considers after 8:00 p.m. CST to be off-peak hours.

6) Item 7.16 is being added to read:

Vendor shall provide next-day cut-over support.

7) Item 7.17 is being added to read:

Vendor shall provide after hours and day two support for the DR site. DOM will coordinate to ensure but considers after 8:00 p.m. CST to be after hours.

8) Item 16 is being amended as follows:

Vendor must deliver the response to Error! Reference source not found. **at ITS no later than ~~Wednesday~~ Monday, March 31 ~~29~~, 2021 at 3:00 P.M. (Central Time).** Responses may be delivered by hand, via regular mail, overnight delivery, e-mail, or by fax. Fax number is (601) 713-6380. ITS WILL NOT BE RESPONSIBLE FOR DELAYS IN THE DELIVERY OF PROPOSALS. It is solely the responsibility of the Vendor that proposals reach ITS on time. Vendors should contact **Error! Reference source not found.** to verify the receipt of their proposals. Proposals received after the deadline will be rejected.

Vendor must include in their proposal a response to each amended requirement as listed above. Vendor must respond using the same terminology as provided in the original requirements.

The following questions were submitted to ITS and are being presented as they were submitted, except to remove any reference to a specific vendor. This information should assist you in formulating your response.

Question 1: Section 4.10 of the LOC states "It is the State's intention that one firewall ship to DOM located at 550 High Street, Jackson, Mississippi on or before May 28, 2021. After the Vendor migrates the data from the existing firewalls, Vendor will deliver and install one firewall to the State Data Center located at 3775 Eastwood Drive, Jackson, Mississippi." This section lists a single firewall to be delivered to DOM, old FW's migrated to single FW, and then single FW moved to ITS. Where will the 2nd FW reside, and who is responsible for setting it up?

Response: **Vendor will be required to install and setup both firewalls. The first firewall will be setup and installed at DOM located at 550 High Street, Jackson, Mississippi. Once this firewall has been setup and data has been migrated, the second firewall will be setup and installed at the State Data Center located at 3775 Eastwood Drive, Jackson, MS.**

Question 2: Where are the two Cisco Firewalls today, and are they under support with Cisco?

Response: **One firewall is located at DOM and one is located at the State Data Center. Neither firewall is under support nor do they qualify for support from Cisco.**

Question 3: Section 5.4.6 of the LOC states, "Able to connect to 10Gb and 40Gb network connections". Do both 40Gb and 10Gb SFP's need to be included, and how many of each or just support 10 and 40 out of the box?

Response: **10Gb SFPs should be supplied with the ability to move to 40Gb as the agency advances with technology.**

Question 4: If just supporting what is the preferred connection on day 1, 10Gb or 40Gb?

Response: **DOM requests 10Gb connection on day one.**

Question 5: Who is responsible for the connection on the DOM and ITS switch end and configuration?

Response: **The Vendor will be responsible for installation and configuration.**

Question 6: What switches and available ports will these be connecting to?

Response: **Connection will be to Cisco 6509 switches. Ports are to be determined.**

Question 7: Section 5.4.10.1 of the LOC states "Vendor shall propose two Next Generation firewalls (proposed firewalls working as a High Availability pair totaling four firewalls)." Are we two propose two HA pairs for a total of 4 firewalls OR two firewalls in a HA setup with one at DOM and one at ITS. Section 4.10 states one FW at each site. This section states two firewalls and then in () four firewalls. Please clarify total number of firewalls.

Response: **See Clarification Number 2 above.**

Question 8: If a total of two firewalls with one at DOM and one at ITS how is the heartbeat for HA established? What is the connection between the DC's and who controls the routing?

Response: **The traffic is using a layer 2 route to establish the heartbeat. ITS controls the routing for the agency and DOM receives a layer 2 hand-off.**

Question 9: Section 5.7.1 of the LOC states "Proposed solution must be capable of being monitored by DOM's primary monitoring solution." What is DOM's primary monitoring solution?

Response: **DOM's primary monitoring solution is AT&T SIME monitoring.**

Question 10: Section 7.11.3.1 of the LOC states "The vendors proposed engineer or engineers should have at least a CISSP (Certified Information Systems Security Professional). Vendor must submit proof of the proposed engineer(s) certification." Is every member of the implementation team required to carry a CISSP certification? EX: Network engineer may assist with any switch work and would not carry the CISSP.

Response: **No. Certification is not required for every member of the team, but at least one team member should carry the certification.**

Question 11: Section 7.12.4 of the LOC states "Successful activation of all new next generation features in the primary datacenter without any service disruption." Please note that any change from one Firewall manufacturer to another would require some

downtown and thus service disruption. We would need to understand DOM's policy and requirements for this.

Response: **The cut-over will be coordinated between ITS and DOM to limit the impact on production traffic.**

Question 12: Item 5.4.6: With the Firewall being able to support 10GB and 40GB connections, how is MDOM planning to connect these appliances into the existing network?

Response: **DOM will use STPs to connect to the switching environment.**

Question 13: Item 5.4.6: Will connectivity be 10GB or 40GB or Both?

Response: **10Gb SFPs should be supplied with the ability to move to 40Gb as the agency advances with technology. DOM requests 10Gb connection on day one.**

Question 14: Item 5.4.6: Will connections be using Optics and Jumpers or DAC/TwinAX/QSFP cables?

Response: **Optics cables will be used for connections.**

Question 15: Item 5.4.6: What switches will the firewalls be connecting to at each Data Center?

Response: **Connection will be to Cisco 6509 switches.**

Question 16: Item 5.4.10.1: What will the HA Firewall Pair connect to at each site upstream and downstream?

Response: **The HA Firewall Pair will connect via a layer 2 switching environment.**

Question 17: Item 5.4.10.1: What are the total number of utilized interfaces on the current firewall?

Response: **Currently, there are three utilized interfaces.**

Question 18: Item 5.4.10.1: Is there a transit network between the current firewall and core infrastructure?

Response: **No.**

Question 19: Item 5.4.10.1: Where are the current SVI's (Switch virtual interface) located? (ex. Are located on current FW or Core switches?)

Response: **The current SVIs are located on core switches.**

Question 20: Item 5.4.10.2: What features (IPS, URL Filtering, Application Visibility, and Advanced Malware Protection) are required to be configured on new HA Firewall pair?

Response: **Vendor should propose all available features. DOM will determine the required features during the final review of proposals.**

Question 21: Item 5.4.10.2: How many firewall rules, NATs, VPN tunnels?

Response: **DOM currently has 2,800 firewall rules, 314 NATs, and 1 VPN tunnel.**

Question 22: Item 5.4.10.2: Would you want to have current firewall configuration sanitized for rules that are no longer in use prior to migration?

Response: **Yes. The current firewall configuration would need to be sanitized.**

Question 23: Item 5.4.10.2: Is there a DMZ configured at either or both sites?

Response: **No. DOM has no DMZs configured at either location.**

Question 24: Item 5.4.10.2: Are there multiple DMZ's configured at each location?

Response: **No. DOM has no DMZs configured at either location.**

Question 25: Item 5.6: How many AD Domains will associate to the Firewalls?

Response: **DOM has one AD that is currently configured on Azure AD.**

Question 26: Item 7.12: Can you please provide more detail on the process of the proof of concept?

Response: **To prove that the firewalls are installed correctly, the awarded solution will be installed behind the current firewall environment in transparent mode to verify the ruleset and features function correctly.**

Question 27: Item 7.12: Is the intent to install one side of the project and then once approved, install the other side?

Response: **DOM anticipates the new firewalls will be up and tested in parallel prior to the decommissioning of the current firewalls.**

Question 28: Item 7.12: Will a CP1/purchase order be issued for the entire project and the Proof of Concept will be considered a first milestone of the project? Please explain the flow of the procurement process.

Response: **After an Award is made, contract negotiations will begin. Once a contract is executed, ITS will issue DOM a CP-1 to give DOM purchase approval to issue a Purchase Order. The first phase of the implementation will include migrating from the existing firewall solution in DOM's primary Data Center as a proof of concept. Following acceptance of each successful firewall install, DOM will provide payment of installation and equip.m.ent according to the terms and conditions of the negotiated contract.**

Question 29: Item 7.12.1: What will the HA Firewall Pair connect to at each site upstream and downstream?

Response: **The HA Firewall Pair will connect via a layer 2 switching environment.**

Question 30: Item 7.12.1: What are the total number of utilized interfaces on the current firewall?

Response: **Currently, there are three utilized interfaces.**

Question 31: Item 7.12.1: Is there a transit network between the current firewall and core infrastructure?

Response: **No.**

Question 32: Item 7.12.1: Where are the current SVI's (Switch virtual interface) located? (ex. Are located on current FW or Core switches?)

Response: **The current SVIs are located on core switches.**

Question 33: Item 7.12.3: What is the code level on current firewall?

Response: **The current level is 8.4(7)23.**

Question 34: Item 7.12.3: What features (IPS, URL Filtering, Application Visibility, and Advanced Malware Protection) are required to be configured on new HA Firewall pair?

Response: **Vendor should propose all available features. DOM will determine the required features during the final review of proposals.**

Question 35: Item 7.12.3: How many firewall rules, NATs, VPN tunnels?

Response: **DOM currently has 2,800 firewall rules, 314 NATs, and 1 VPN tunnel.**

Question 36: Item 7.12.3: Would you want to have current firewall configuration sanitized for rules that are no longer in use prior to migration?

Response: **Yes. The current firewall configuration will need to be sanitized.**

Question 37: Item 7.12.3: Is there a DMZ configured at either or both sites?

Response: **No. DOM has no DMZs configured at either location.**

Question 38: Item 7.12.3: Are there multiple DMZ's configured at each location?

Response: **No. DOM has no DMZs configured at either location.**

Question 39: Can a scrubbed firewall configuration be provided?

Response: **No.**

Question 40: Conversion format? Rebuild? Redesign?

Response: **This will qualify as a redesign, as "clean up" of the current rule-set is expected.**

Question 41: Platforms migrating from and to?

Response: **Migration will be from and to a Cisco ASA.**

Question 42: Current version of software?

Response: **The current level is 8.4(7)23.**

Question 43: Security features currently provided by existing firewall? (Content filtering, IPS, etc.) Are these to be migrated?

Response: **The current firewall features Web Cache Communication Protocol (WCCP) for EOL Ironport and should be migrated.**

Question 44: Additional features currently provided by existing firewall? (VPN, dynamic routing, etc.)

Response: **The current firewall has no additional features installed.**

Question 45: Number of physical interfaces in use by the current firewall?

Response: **There are three utilized interfaces.**

Question 46: Is the mapping of physical ports from the current firewall to the FortiGate defined? Are there enough physical ports / transceivers?

Response: **DOM has Cisco firewalls. This question is not applicable.**

Question 47: Number of VLAN interfaces that are used in the current firewall?

Response: **There are three utilized interfaces.**

Question 48: Will VLANs concentrate / distribute on LAG interfaces?

Response: **No. VLNs are controlled by core switching.**

Question 49: How many LAGs will be used?

Response: **There are no LAGs in use today. See Clarification Number 3 above.**

Question 50: Are those the same ones that are currently defined?

Response: **There are no LAGs in use today. See Clarification Number 3 above.**

Question 51: Number of address objects and groups?

Response: **There are currently 630 address objects and groups.**

Question 52: Number of service objects and groups?

Response: **There are currently 39 service objects and groups.**

Question 53: Number of NAT objects/policies?

Response: **There are currently 314 NAT objects/policies.**

Question 54: Number of firewall policies?

Response: **There are currently 2,800 firewall policies.**

Question 55: Number of site-to-site VPNs to migrate?

Response: **DOM has one VPN to migrate.**

Question 56: GRE being used?

Response: **Generic Routing Encapsulation (GRE) is not being used.**

Question 57: Pre-shared keys or certificates?

Response: **Pre-shared keys are in use for the site-to-site VPN tunnel.**

Question 58: Number of client remote access VPNs to migrate? Type(s)? Number of users/groups?

Response: **There will be one site-to-site VPN tunnel to migrate based on the current configuration, IPSEC type. There are currently two users/twenty groups.**

Question 59: Type of user authentication? Two factor authentication?

Response: **DOM has no user authentication or two factor authentication.**

Question 60: What type of dynamic routing is currently in use?

Response: **This question is not applicable.**

Question 61: BGP: How many AS, neighbors?

Response: **This question is not applicable.**

Question 62: Are there route-maps?

Response: **This question is not applicable.**

Question 63: OSPF: How many areas?

Response: **There are currently 82 OSPF areas.**

Question 64: Is there any kind of filtering for route propagation?

Response: **No. There is no kind of filtering for route propagation.**

Question 65: Operational modes of FortiGate firewall:

Response: **DOM has Cisco firewalls. The modes will be Layer-2/Transparent.**

Question 66: Are new features being added?

Response: **Security Fabric and Fabric Connectors will be added.**

Question 67: Are new security features being implemented?

Response: **Web Content Filtering, IPS, Deep Packet Inspection, and IDS will be implemented.**

Question 68: Authentication requirements for single-sign on?

Response: **The current firewall does not have any authentication requirements.**

Question 69: Will additional agents be required? (Citrix, Terminal Services, etc.)

Response: **No additional agents are required by DOM.**

Question 70: Number of Active Directory Domain Controllers?

Response: **DOM has three on-premise AD controllers and utilizes Azure AD.**

Question 71: Number of users/groups?

Response: **There are currently two users/twenty groups.**

Question 72: Is any additional configuration required?

Response: **Yes. The Vendor will need to look at the configuration and, if not Cisco, remove the parts of the configuration related to Cisco and recommend best practices on the configuration moving forward. The firewalls and services will be configured to run the rules that DOM needs.**

Question 73: Is after hours configuration required?

Response: **Yes. See Clarification Number 5 above.**

Question 74: Is cut-over support required?

Response: **Yes. See Clarification Number 6 above.**

Question 75: Is next day cut-over support required?

Response: **Yes. See Clarification Number 6 above.**

Question 76: Is after hours & day 2 support required for the DR site?

Response: **Yes. See Clarification Number 7 above.**

LOC responses are due Wednesday, March 31, 2021, at 3:00 p.m. (Central Time).

If you have any questions concerning the information above or if we can be of further assistance, please contact Jill Chastant at 601-432-8214 or via e-mail at jill.chastant@its.ms.gov.

cc: ITS Project File Number 46217-B